(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN JPA 10-285381

(11) Publication number: **10285381 A**

(43) Date of publication of application: **23.10.98**

(51) Int. Cl **H04N 1/387**
G06T 1/00
G09C 5/00

(21) Application number: **09084990**

(22) Date of filing: **03.04.97**

(71) Applicant: **MATSUSHITA GRAPHIC COMMUN SYST INC**

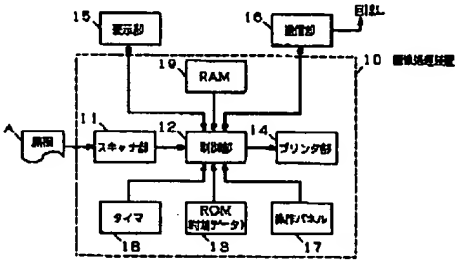
(72) Inventor: **UCHIDA SHIGERU**

(54) **IMAGE-PROCESSING UNIT**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an image-processing unit, where the authentication capability is considerably enhanced by specifying the operator or a device on the occurrence of forgery of a paper money or the like, so as to enable tracing of under which circumstance the forgery is conducted.

SOLUTION: This processing unit is provided with a scanner section 11 that reads an image on an original, a ROM 13 that stores electronic watermark data added to image data outputted from the scanner section 11 by which a device in use or the user is identified, a control section 12 for applying additional processing to image data of the watermark data stored in the ROM 13, and an interface means for outputting the image data with the watermark data added to them to a printer section 14 or a communication section 16.



THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－285381

(43)公開日　平成10年(1998)10月23日

(51)Int.Cl.[6]	識別記号	ＦＩ	
H04N 1/387		H04N 1/387	
G06T 1/00		G09C 5/00	
G09C 5/00		G06F 15/66	B

審査請求　未請求　請求項の数６　ＯＬ　（全６頁）

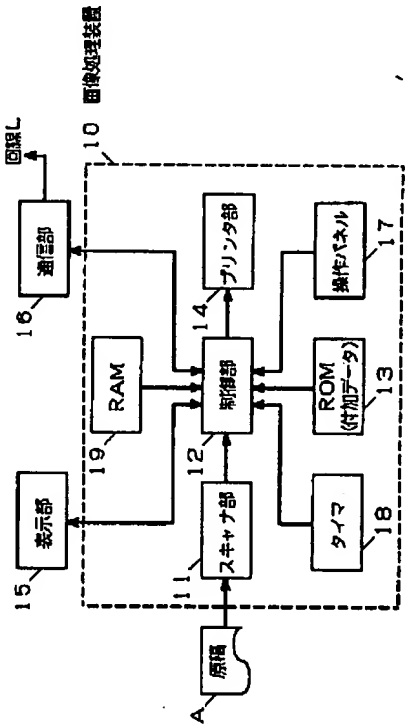
(21)出願番号　特願平9－84990

(22)出願日　平成９年(1997)４月３日

(71)出願人　000187736
松下電送システム株式会社
東京都目黒区下目黒２丁目３番８号
(72)発明者　内田　茂
東京都目黒区下目黒２丁目３番８号　松下電送株式会社内
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】画像処理装置

(57)【要約】
【課題】　紙幣等の偽造発生時点での操作者あるいは装置の特定し、どのような状況で偽造が行われたか追跡を可能とし、偽造抑止力を大幅に高めた画像処理装置を提供する。
【解決手段】　原稿上の画像を読取るスキャナ部１１と、このスキャナ部１１から出力される画像データに付加され、使用された装置あるいは使用者を識別可能にする電子的な透かしデータを格納するＲＯＭ１３と、このＲＯＭ１３に格納された透かしデータの画像データに対する付加処理を行う制御部１２と、透かしデータの付加された画像データをプリンタ部１４あるいは通信部１６に出力させるためのインターフェース手段を備える。



1

【特許請求の範囲】

【請求項１】　原稿上の画像を読取る読取手段と、この読取手段から出力される画像データに付加され、使用された装置を識別可能にする電子的な透かしデータを格納する記憶手段と、この記憶手段に格納された透かしデータの画像データに対する付加処理を行う制御手段と、前記透かしデータの付加された画像データを出力させるためのインターフェース手段とを備えた画像処理装置。

【請求項２】　原稿上の画像を読取る読取手段と、この読取手段から出力される画像データに付加され、操作者を識別可能にする電子的な透かしデータを格納する記憶手段と、この記憶手段に格納された透かしデータの画像データに対する付加処理を行う制御手段と、前記透かしデータの付加された画像データを出力させるためのインターフェース手段とを備えた画像処理装置。

【請求項３】　前記インターフェース手段は通信回線等を介してネットワーク上に出力させるための機能を有することを特徴とする請求項１または２記載の画像処理装置。

【請求項４】　使用された装置を識別可能にする電子的な透かしデータが付加された原稿画像データを入力する入力手段と、この入力手段から入力された画像データから前記透かしデータの抽出処理を行う制御手段と、この制御手段により抽出された前記透かしデータを表示させるためのインターフェース手段を備えた画像処理装置。

【請求項５】　操作者を識別可能にする電子的な透かしデータが付加された原稿画像を入力する入力手段と、この入力手段から出力される画像データから前記透かしデータの抽出処理を行う制御手段と、この制御手段により抽出された前記透かしデータを表示させるためのインターフェース手段を備えた画像処理装置。

【請求項６】　前記入力手段は通信回線等を介して接続されるネットワーク上からの画像データを入力するものであることを特徴とする請求項４または５記載の画像処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像処理装置、特にカラー画像を読み取って、複写／通信等を行う画像処理装置に関するものである。

【０００２】

【従来の技術】近年、ファクシミリを始めとする各種画像処理装置の機能あるいは性能の増大にはめざましいものがあり、そのひとつとして、カラー画像を元原稿の色に極めて忠実に再現しつつ複写、記録または通信できる画像処理技術があり、またかかる技術を用いた画像処理装置の低価格化が実現しつつある。一方、紙幣を扱う自動両替機、自動販売機、あるいは自動金銭取扱機等が普及し、紙幣を複写装置で複写し、これを用いる犯罪が可能な状況ができつつあり、本物の紙幣であるか複写された紙幣であるかを人が見ても区別することが困難な状況になりつつある。

2

【０００３】そこで、近年のこの種のカラー画像処理装置では、紙幣認識・偽造追跡という偽造防止機能で対策することが行われていた。（参考文献　日経エレクトロニクス1992.12.21 NO.570、特公平６－５０９０１）

以下、従来の技術を図面を用いて説明する。図４は、従来技術の画像処理装置を示すブロック図である。図４において、Ａは複写等の画像処理を行う対象物である原稿である。１は該原稿の画像を読取るスキャナである。２はスキャナ１で読取られた画像データを処理し、原稿が紙幣等の画像処理を行って良いものかそうでないものかを判断するＣＰＵ等を含む判断部である。３は判断部２が判断するために用いる学習機能を持つ画像メモリを有する辞書回路である。４は判断部２からの情報を元に信号を出力する信号発生回路である。

【０００４】以上のように構成された従来の画像処理装置について動作を説明する。まず、複写される原稿の情報をイメージセンサであるスキャナ１で光電変換しその情報を判断部２に渡す。判断部２では、パターンマッチング等の手法を用い、あらかじめ紙幣のデータが蓄積されている辞書回路３と渡された画像データとを比較判定する。判断部２の情報をもとに、信号発生回路４では、紙幣と判断された場合、複写等の動作を中断する信号を発生させ、また、紙幣と判断されない場合は、複写等の動作を継続させる信号を発生させ、複写動作の制御を行っていた。

【０００５】さらに、従来より追跡を行う技術として、紙等の複写物に人間の目では見えないインク等を用い、複写に用いた装置を特定するするための方法も偽造防止技術のひとつの手段として知られている。

【０００６】

【発明が解決しようとする課題】しかし、上述の従来技術の構成では、辞書回路に未登録の紙幣や有価証券では偽造防止が働かないことや、偽造追跡では紙以外の複製には有効でないなど、犯罪の抑止という点で完全ではないという問題が発生していた。

【０００７】また、技術進歩により手軽に複写できるため、弾み、興味本位での偽造がやりやすく、より確実な偽造防止策が求められているという問題も発生していた。

【０００８】本発明は、上述の問題点に鑑みて為されたもので、その目的は偽造発生時点での操作者あるいは装置の特定し、どのような状況で偽造が行われたか追跡を可能とし、偽造抑止力を大幅に高めた画像処理装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明は、上述の目的を達成するため、入力画像に対して操作者、装置を特定するための電子的な透かし情報を付加する機能と抽出する

機能を備えたことを特徴とするものである。そして、本発明は上述の構成により、透かし情報を電子データとして画像データに付加され、しかも、透かし情報のみを抽出することができるので、紙幣等の偽造防止及び偽造抑止に効果的である。

【００１０】請求項１に記載の発明は、原稿上の画像を読取る読取手段と、この読取手段から出力される画像データに付加され、使用された装置を識別可能にする電子的な透かしデータを格納する記憶手段と、この記憶手段に格納された透かしデータの画像データに対する付加処理を行う制御手段と、前記透かしデータの付加された画像データを出力させるためのインターフェース手段とを備えたものである。これにより、偽造複製が発生した場合でも、どの装置で処理されたかを識別可能にする非可視的な透かしデータを残すことができる。

【００１１】請求項２に記載の発明は、原稿上の画像を読取る読取手段と、この読取手段から出力される画像データに付加され、操作者を識別可能にする電子的な透かしデータを格納する記憶手段と、この記憶手段に格納された透かしデータの画像データに対する付加処理を行う制御手段と、前記透かしデータの付加された画像データを出力させるためのインターフェース手段とを備えたものである。これにより、偽造複製が発生した場合でも、誰が処理したものかを識別可能にする非可視的な透かしデータを残すことができる。

【００１２】請求項３に記載の発明は、請求項１または２に記載の発明に加え、インターフェース手段に通信回線等を介してネットワーク上に出力させるための機能を備えたものである。これにより、ネットワーク上の第三者に画像データが出力される場合でも、非可視的な透かしデータを残すことができる。

【００１３】請求項４に記載の発明は、使用された装置を識別可能にする電子的な透かしデータが付加された原稿画像データを入力する入力手段と、この入力手段から入力された画像データから前記透かしデータの抽出処理を行う制御手段と、この制御手段により抽出された前記透かしデータを表示させるためのインターフェース手段を備えたものである。これにより、偽造複製による画像データが入力された場合でも、どの装置で処理したものかを識別することができる。

【００１４】請求項５に記載の発明は、操作者を識別可能にする電子的な透かしデータが付加された原稿画像を入力する入力手段と、この入力手段から出力される画像データから前記透かしデータの抽出処理を行う制御手段と、この制御手段により抽出された前記透かしデータを表示させるためのインターフェース手段を備えたものである。これにより、偽造複製による画像データが入力された場合でも、誰がで処理したものかを識別することができる。

【００１５】請求項６に記載の発明は、請求項４または５に記載の発明に加え、入力手段が通信回線等を介して接続されるネットワーク上からの画像データを入力するものであることを特徴とする。これにより、ネットワーク上の第三者からの画像データを入力する場合でも、非可視的な透かしデータから識別が可能となる。

【００１６】

【発明の実施の形態】以下、本発明の一実施例について図面を参照して説明する。

【００１７】図１は、本発明の一実施例による画像処理装置の概略を示すブロック図である。図１において、Ａは複写等の画像処理を行う対象物の原稿である。１０は画像処理装置を全体を示しており、１１は原稿Ａの情報を読取って電子データに変換する読取手段あるいは入力手段としてのスキャナ部である。１２は１１で読取られたデータを入力し、電子透かしデータを付加処理あるいは抽出処理を制御する制御部である。１３は電子透かしデータが格納された読出し専用のメモリ（ＲＯＭ）である。１４は制御部１２によって電子透かしデータの付加された画像データを紙に出力するプリンタ部である。１５は図示しないインターフェースを介して画像処理装置１０と外部接続される表示部であり、表示部１５においては、画像データの中から抽出された電子透かしデータを可視的に表示される。１６は制御部１２のインターフェース手段としての通信部であり、制御部１２によって処理される画像データについて回線Ｌを通じてネットワーク上に接続された所望の宛先と送受信を行う。なお、１７は読取動作、記録動作等の各種処理の実行指示を与える操作パネルであり、１８は装置への時刻表示、動作制御等を行うためのタイマである。また、１９は画像処理時に必要な作業領域として割り当てられるメモリ（ＲＡＭ）である。

【００１８】以上のように構成された画像処理装置について、以下その動作を説明する。まず、操作パネル１７から原稿Ａを複写するための指示入力を行うと、原稿Ａの画情報がスキャナ部１１で光電変換されて画像データとして制御部１２に出力される。そして制御部１２では、原画像の画質を低下させることなく、原稿Ａの画像データに対してＲＯＭ１３に格納された付加データの埋め込み処理を行う。付加データの埋め込まれた画像データは画像処理装置１０内ではプリンタ部１４により紙等の媒体へ出力することができる。ここで、画像データが出力された紙には、プリンタ部１４に出力された画像自体に人間の目には見えないような非可視的な形で、付加データが埋め込まれている。この人間の目には見えない形の付加データは、後述する制御部１２の機能の１つである電子透かしリーダーと呼ばれるソフトウェア処理によって付加データの抽出、解析を行うことができる。ここで、抽出、解析される付加データとして、複写に用いた装置、あるいは操作者を特定するようなデータを用いることにより、偽造追跡を迅速かつ効率良く行うことが

でき、最終的に偽造防止の効果が高められる。

【００１９】ところで、電子透かしの付加技術は、画像のディジタル化とインターネットの普及が進んだことで、注目され始めている。電子透かしの付加技術は、とりわけパソコン等を使ったディジタル著作物の複製を制限するために効果的であり、電子透かしは英語ではＷａｔｅｒ Ｍａｒｋ（ウオーターマーク）とよばれ、特開平８－２４１４０３に示されるような関連出願が存在する。また、画像処理ソフトＰｈｏｔｏｓｈｏｐ Ｖｅｒ．４ （ＵＳＡ、Ａｄｏｂｅ社製）の中に一部の機能としても使用されている。

【００２０】これらの電子透かしデータの付加技術によれば、スキャナ等から読み込まれた画像データ（多くの場合Ｒ／Ｇ／Ｂのデータ形式）に、単純に電子透かしデータ付加する方法が一般的である。しかしながら、単純付加では色情報が変化し、人間は色が変わったと知覚してしまう。そこで、スキャナからのデータをＬ＊ａ＊ｂ＊等の輝度情報と色度情報とで構成される色空間に変換し、輝度情報のみに付加データを埋め込み、色度情報は変えないようにするのが好ましい。

【００２１】ところで、人間の輝度に対する特性は暗い情報の変化には感度が高く、明るい情報の変化には感度が低いため、明るい部分にデータを付加すると、付加情報の識別が人間の目では困難になる。さらに画像全体にデータをランダムに付加したり、画像の単調な部分と精細な部分とのどちらでも目につかないようにデータ付加の強度を変えることにより、様々なデータ加工に対し耐久性が向上し、編集・複写・印刷等を経ても埋め込まれたデータは欠落することなく確実に付随させてゆくことができる。

【００２２】次に、本発明の実施例における付加データの内容について説明する。付加されるデータは、偽造防止の効果を高めるため、次のような情報を適宜選択して付加される。

【００２３】(1) 装置製造番号

(2) 発信元印字データ：会社名、主たる使用者等の装置設置時に前述のデータ入力なしでは動作しないようにしておくことにより、確実にデータ入力される。

【００２４】(3) 複写データ作成日時

(4) 複写データ提供元：内部／外部、外部の場合通信であれば電話番号やe-mailアドレス等、ＰＣであればユーザ名等。

【００２５】さらに、より確実なデータとして次のものがある。

(5) 指紋データ：複写開始ボタンに、指紋認識装置を内蔵することにより実現可能である。

【００２６】(6) 使用者の顔画像データ

最近、小型でかつ安価になったＴＶカメラを装置に接続することにより実現可能である。

【００２７】上述のデータのうち、(1)から(4)まではデータ量自体が比較的小さく、容易に付加することができる。

【００２８】また、(5)や(6)はデータ量は多いものの、データ自体で直接、偽造作成者を特定できるものであり、偽造抑止の効果は絶大である。

【００２９】次に、上述本発明の実施例における付加を用いた追跡動作について、図２をもとにその手順を説明する。偽造物には紙へ作成された偽造書類Ｂや電子データであるフロッピーディスクＣの媒体や外部からのデータである通信データＤがある。紙データである偽造書類Ｂの場合は先ずスキャナ部１１に読み込ませて電子データへ変換する。これの電子データは、制御部１２の機能の１つである電子透かしリーダーと呼ばれるソフトウェア処理によって付加データの抽出、解析が実行される。なお、この電子透かしリーダ２０を、一般のパーソナルコンピュータのアプリケーションとして動作させ、付加データの抽出、解析処理が実行させるようにしてもよい。このデータ処理は上述の制御回路１２における電子透かしの付加処理と逆の処理動作を行い、スキャナ１１から送られたデータを付加データ２１と画像データ２２とに分離する。分離された付加データ２１はディスプレイ等の表示部１５にて表示される。図3は、各種透かしデータを用いた表示例を示したものであり、画像データに透かしデータが非可視的に埋め込まれたオリジナル画像と透かしデータを抽出した表示例とを対比して示してある。（ａ）は装置製造番号の透かしデータ、（ｂ）は発信元印字データと複写データ作成日時の透かしデータ、（ｃ）は複写データ提供元の透かしデータ、（ｄ）は指紋データの透かしデータ、（ｅ）は使用者の顔画像データの透かしデータをそれぞれ表わしている。これらの透かしデータは追跡調査の重要なデータとして用いられる。例えば、偽造に使用した装置製造番号や発信元印字データから偽造に使用した装置の設置会社名、主たる使用者等や偽造日時、偽造データ提供元等のデータが可視化されれば迅速な調査が可能になる。

【００３０】電子データであるフロッピーディスクＣ等の媒体や外部からのデータである通信Ｄの場合も上記と同様にして、電子透かしリーダ２０を備えたパーソナルコンピュターへ送り、データ処理を実行する。これらの場合も、以後の処理は同様である。

【００３１】なお、ここまでは主に紙幣偽造を念頭に説明したが、手形や株式証券、小切手、トラベラーズチェック等の有価証券類の偽造防止にも全く同様の手段によって適用可能となる。

【００３２】また、画像入力と画像出力とが通信回線等ネットワーク上でデータの転送が行われる場合でも、常に電子透かしデータが付加されて転送されるので、画像出力時点で追跡動作を開始することができ、同様の効果を期待できることは言うまでもない。

【００３３】

7

【発明の効果】以上の説明から明らかなように、本発明は、入力画像に対して操作者、装置を特定するための電子的な透かし情報を付加する機能と抽出する機能を備えたので、各種媒体に非可視的な情報を画像と一体化させ偽造追跡を可能にすることにより、偽造防止・偽造抑止の効果を大幅に向上させることができる。

【００３４】また、付加データは紙媒体のみならず電子媒体にも付加可能なため、近年身近になってきたパーソナルコンピュータとスキャナとプリンタとによる偽造にも対応でき、偽造抑止の効果を大幅にあげることができる。

【００３５】また、付加データをさらに高度化し、指紋・顔画像データ等を使用することにより偽造犯人の直接検挙を可能にするため、偽造抑止の効果を大幅にあげることができる。

【図面の簡単な説明】

【図１】本発明の一実施例による画像処理装置のブロック図

【図２】本発明の一実施例における追跡を説明するフロー図

8

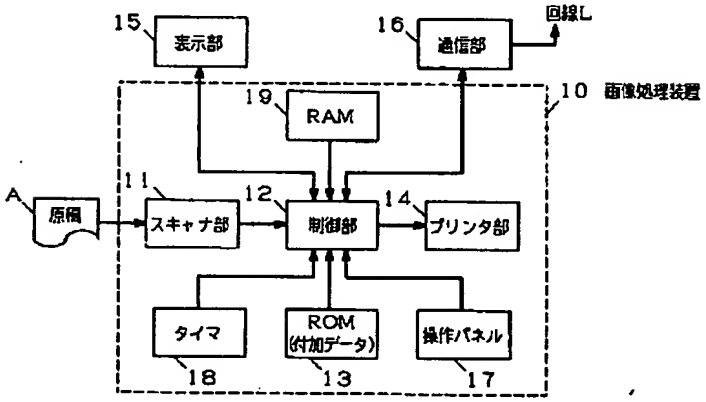
【図３】各種透かしデータを用いた表示例を示す図

【図４】従来例の構成を示すブロック図

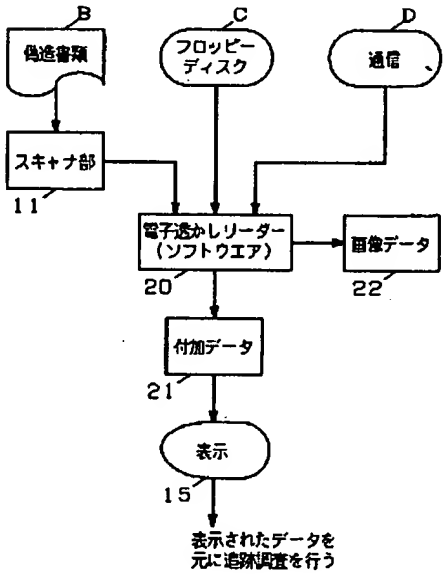
【符号の説明】

Ａ　原稿
Ｂ　偽造書類
Ｃ　フロッピーディスク
Ｄ　通信データ
１１　スキャナ部
１２　制御部
１３　ＲＯＭ（付加データ）
１４　プリンタ部
１５　表示部
１６　通信部
１７　操作パネル
１８　タイマ
１９　ＲＡＭ
２０　電子透かしリーダー
２１　付加データ
２２　画像データ

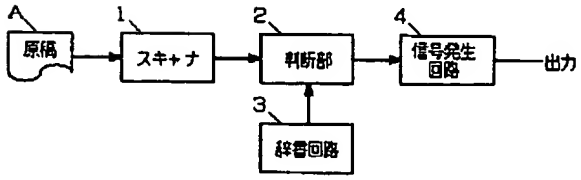
【図１】



【図２】



【図４】



【図３】